NextGen
Application Service Provider Privacy & Security Policies

Access

All items when introduced to the Tellurian datacenter environment have the potential to bring along with them unwanted foreign matter such as dust, dirt, and especially metallic or conductive powders, fibers, or shavings. Effective immediately, no packages or servers from outside the Tellurian datacenter are to bebrought into the facility without following the checklist below:

1. ALL equipment is to be moved directly from the loading dock or entrance door(s) to a separate, pre-designated “staging” area for de-skidding and de-boxing. After equipment has been removed from its packaging, it may be brought into the datacenter machine room for installation in a rack.

Unpacking and de-skidding of equipment is not allowed within the datacenter room in order to maintain a clean room environment. The Tellurian datacenter operations staff is available for assisting with any questions regarding this process. Absolutely all packaging must be removed from any items to be brought into the datacenter area. Cardboard and paper are fire hazards and are not allowed. The removal of such packaging must be performed in a staging area OUTSIDE the datacenter. It is the responsibility of ALL employees with datacenter access privileges to ensure this rule is followed at all times. Failure to comply will result in discipline up to and including termination of employment.

2. Any equipment which is not factory new must be taken outdoors downwind from the datacenter and blown out thoroughly and disassembled as needed to ensure the interior and all exterior surfaces are completely free of any foreign substance or material including dust. If the equipment is not able to be cleaned completely, it is not permitted to be taken into the datacenter. Contact sales to help client obtain new equipment.

3. The Tellurian datacenters are high velocity and high volume airflow environments. Any small quantity of contaminants will be dispersed quickly and efficiently throughout the entire facility which may lead to catastrophic failure. Therefore the following are absolutely banned with zero exceptions: all fibrous materials – carbon fiber mats/blankets/sheets, steel/copper/brass wool or electrically conductive materials of any type which are smaller than 5mm x 5mm (1/8” x 1/8”).

4. All contractor equipment must be inspected by a Tellurian engineer to look for prohibited materials in the staging area prior to granting access to the datacenter.

5. All cutting, drilling, filing, grinding, or any other work performed to ferrous or non-ferrous metals in the datacenter is absolutely prohibited! Any cutting must be performed outside. When it is not possible to work outside, , the work must be performed off hours, the air handlers must be temporarily stopped, cardboard and plastic placed over any racks in the work area and a vacuum used at all times to capture as many particles as possible.

6. All non-emergency contractor work must be performed between 11PM and 7AM local time unless approved in advance by the CEO and then the contractor must be escorted at all times.

7. All contractors must sign a statement of agreement which says they have read and understand the datacenter rules and accept full liability for any violation of the rules.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Authorization	Access to the Tellurian hosted client systems via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase or Active Directory integrated VPN access via Cisco VPN client software with a client unique access group and password.
Authentication	Access to the Tellurian hosted client systems via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase or Active Directory integrated VPN access via Cisco VPN client software with a client unique access group and password.
Audit	**3.3 Monitoring** • All security-related events on critical or sensitive systems must be logged and audit trails saved as follows: o All security related logs will be kept online for a minimum of 1 week. o Daily incremental tape backups will be retained for at least 1 month. o Weekly full tape backups of logs will be retained for at least 1 month. o Monthly full backups will be retained for a minimum of 2 years. • Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to: o Port-scan attacks 31 o Evidence of unauthorized access to privileged accounts o Anomalous occurrences that are not related to specific applications on the host. **3.4 Compliance** • Audits will be performed on a regular basis by authorized organizations within Tellurian Networks. • Audits will be managed by the internal audit group or InfoSec, in accordance with the *Audit Policy*. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification. • Every effort will be made to prevent audits from causing operational failures or disruptions. **4.0 Enforcement** Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
Secondary Uses of Data	Neither Tellurian Networks nor NextGen Healthcare participates in any distribution, sale, or any other secondary use of client data.

Data Ownership	The data is always owned by the client, regardless where it resides. Even under circumstance of termination, the client is given a their data.